# Chapter 16:   Kerberized UNIX System Administration Issues

In this chapter we discuss some UNIX system administration issues related to the installation of Kerberos software.

## 16.1 Alterations Made to your System when Fermi Kerberos is Installed

When you issue one of the **`ups install ...`** commands to complete the installation of the **kerberos** product (e.g., see step 5 of section 14.2 *Installing Fermi Kerberos using UPS/UPD*), the following changes are made to your environment:

- new directory `/usr/krb5` and directories/files underneath are created
- some service (port) definitions are added to `/etc/services` (if not already present). Note that these changes must be made known to the system: for Sun and Linux, make sure `/etc/nsswitch.conf` points to the correct `services` file.
- `/etc/krb5.conf` and `/etc/krb5.keytab` files are added
- `/etc/inetd.conf` is altered to enable Kerberized services and disable non-Kerberized ones, then `SIGHUP` is sent to `inetd`[1]. The default kerberos install preserves pre-existing usage of tcpwrappers on a service-by-service basis.
- if **`ups install-keep-ssh`** isn't chosen, `/etc/sshd_config` is also altered

[1] If two **`inetd`** processes are running, some nonKerberized services like rlogin may get handled by a different file than `/etc/inetd.conf` and thus won't be disabled by the **kerberos** installation script as they should be.

## 16.2 Setting Defaults for Tickets/Applications

The /etc/krb5.conf file, described in Chapter 17: *The Kerberos Configuration File: krb5.conf*, contains configuration information needed by the Kerberos V5 library. This includes information describing the default Kerberos realm, and the location of the KDC. You can use it to set default flags for tickets (e.g., forwardable, renewable) and application parameters (e.g., tell application to forward “forwardable” tickets). If your machine is in a domain other than fnal.gov, you’ll need to add your domain to the [domain_realm] section of the file (see section Chapter 18: *Additional UNIX Sysadmin Information for Off-Site Installations*). For complete information, refer to http://www.osxfaq.com/man/5/krb5.conf.html.

Note that as of January 2001, the current krb5.conf file available from KITS does not turn on ticket forwarding by default (for applications that check this file, e.g., **telnet**, **rlogin**, **FTP**, **rsh**). This was changed in response to users’ concerns about inadvertently forwarding credentials to an untrustworthy machine. However if the sysadmin turns it on by editing krb5.conf, a later update or re-installation will leave that change alone.

## 16.3 The /etc/hosts File

In the /etc/hosts file, the first-listed name for the local system must be the full name, including the domain, and must not be a nickname. The line should be of the form:

```
<IP address> <node>.<domain> <node>
```

E.g.,:

```
<131.225.11.11> mynode.fnal.gov mynode
```

or, depending on your home institution, something like

```
<111.111.11.11> mynode.myuniv.edu mynode
```

Note regarding tcpwrappers: If in /etc/hosts.deny there is an entry ALL : ALL, then all tcp connections are disabled, unless explicitly enabled in /etc/hosts.allow.

## 16.4 Portal Mode Configuration

A UNIX host running **kerberos v1_0** or later performs the portal function by default when accessed via telnet or FTP from the untrusted realm, unless this mode is specifically disabled. Host and **FTP** principals must exist for the node in order to enable portal mode.

In the `inetd.conf` file (which resides in either `/etc` or `/etc/inet`) you should find a line for **telnet** similar to:

```
telnet stream tcp nowait root /usr/krb5/sbin/telnetd telnetd
-Pa valid
```

And for **FTP**:

```
ftp stream tcp nowait root /usr/krb5/sbin/ftpd ftpd -aOP
```

The **`P`** flag in these lines enables portal mode. To disable this mode, remove the **`P`** flag. (This still leaves unencrypted **rsh** and **rlogin** open[1].)

## 16.5 Register yourself as an Administrator

If you need to allow remote logins to your machine or offer services, you need host and ftp principals for the machine. First register yourself in the database of system administrators. Go to *System Administrator Registration* at `http://miscomp.fnal.gov/sysadmindb/` to register.

## 16.6 User Accounts and Passwords

### 16.6.1 User Account Names

Set up each user’s account such that the account name (login id) is the same as the person’s principal. Otherwise, the user is subject to the problems listed in C.2 *If your Principal and Login Name do not Match.*

[1] To eliminate those, take out the klogin service from inetd (leave eklogin) and add an ’e’ flag to the kshell service.

### 16.6.2 Determine if a Particular Principal Exists

If you need to check whether a principal has been created for a user, run the **kinit** command with the principal name you want to test. Enter at least one character at the password prompt. The text of the error message will indicate whether the principal exists or not. If the principal exists, it will give a message indicating the password is wrong:

```
% kinit tez
    Password for tez@FNAL.GOV: x
    kinit: Preauthentication failed while getting initial
    credentials
```

If the principal doesn't exist, it will give a "Client not found..." message instead:

```
% kinit tezNOT
    Password for tezNOT@FNAL.GOV: x
    kinit: Client not found in Kerberos database while getting
    initial credentials
```

### 16.6.3 User Passwords

A Kerberized machine uses the Kerberos login program by default, and that login program accepts Kerberos passwords. Standard UNIX passwords can be used for non-Kerberos-authenticated login at the console. If a user will only access the gateway remotely, the user's account doesn't need a local UNIX password. Using `!!` in the password field for that account in `/etc/shadow` will disable local login, while leaving remote Kerberos login available.

Disable NIS passwords and AFS passwords. There should be no passwords in the yp password files. Standard UNIX passwords can be used for non-Kerberos-authenticated login at the console.

### 16.6.4 Providing Access to Sensitive Accounts

You as the system administrator can choose to require that users of the *root* account and/or any other sensitive accounts obtain a *root instance* of their principal. This is described in section 9.4 *Using Root Instance of your Principal*.

To allow authorized users to log in directly to a sensitive account via ssh, telnet, rsh, rlogin or ftp, add the person's principal (or the person's */root* principal if you use that method) to the `.k5login` file in the account's home directory (`/root/` for Linux, `/` for the other supported flavors). This file is described in section 9.3 *Account Access by Multiple Users*.

For the *root* account, an alternative is for the authorized user to log in to the machine under his own login id, and provided he has a forwardable ticket on the machine, he can use **`ksu`** (instead of **`su`**) to run as *root*.

## 16.7 Non-user Accounts

There are often accounts maintained for file ownership/permissions reasons, and people don't log into these accounts. Typically these accounts have names that don't correspond to user names (e.g., "products"), but it is best to prevent accidental login in case a user's principal matches this account name. To do so, create an empty `.k5login` file in the account's home directory (see section 9.3.1 *The .k5login File*).

## 16.8 Searching KDC Log Files and the Principal List

The KDC log files and the list of principals are available in AFS space for users who are registered system administrators (see section 16.5 *Register yourself as an Administrator*). If you are a registered system administrator and can't access the KDC logs as described here, please contact *nightwatch@fnal.gov.*[1]

The AFS directory `/afs/fnal.gov/files/data/k5logs` contains various KDC log files and a list of KDC principals. These files can be used by system administrators to understand error messages and to diagnose problems. All the directories referred to below reside under this directory.

The `princ/`, `kdc/`, `log/` and `adm/` directories contain subdirectories for the year and month. The format for the names of these directories is YYYY-MM (e.g., 2001-08). Under each YYYY-MM directory are the actual log files as listed here:

`princ/` contains the weekly list of KDC principals, plus the `diag_user.pl` which allows you to look at yesterday's log file.

`kdc/` contains the daily KDC transaction log files (the transaction records for each KDC are maintained in separate files)

`log/` contains the daily KDC log files (not much here)

[1] If your AFS username is different than your email username, it's likely that the script that built the AFS group that controls access to the KDC log files doesn't have your correct username and you can't access the files.

`adm/` contains the daily KDC administration log files

The format for the names of the log files in these directories is `i-krb-<n>.YYYY-MM-DD` (e.g.,. `i-krb-3.2001-08-15`). The meaning of `i-krb-<n>` is the DNS CNAME for a KDC as follows:

i-krb-2 Pilot realm (PILOT.FNAL.GOV) master KDC (alias krb-pilot-1)

i-krb-3 Production realm (FNAL.GOV) master KDC (alias krb-fnal-1)

i-krb-4 FNAL.GOV realm backup KDC (alias krb-fnal-2)

i-krb-5 PILOT/FNAL realm backup located in D0 (alias krb-fnal-5, krb-pilot-3)

i-krb-6 PILOT/FNAL realm backup located in CDF (alias krb-fnal-4, krb-pilot-4)

i-krb-7 PILOT/FNAL realm backup located in BD (alias krb-fnal-3, krb-pilot-5)

i-krb-8 FNAL realm backup located in Soudan (alias krb-fnal-6)

The list of principals under the `princ/` directory is only maintained for the master KDCs, i-krb-2 and i-krb-3. The list of principals includes the attributes for each principal and the expiration dates for the principal and password. Each principal record has comma-separated fields. The format of the records is as follows:

| Field number | Field value | Description |
|---|---|---|
| 1 | principal name | full principal name including realm |
| 2 | principal expiration | number of days till principal expires, "*" for no expiration, "E" for expired |
| 3 | password expiration | same as for principal expiration |
| 4 and beyond | principal attributes | |

Most principal attributes are self explanatory such as “DISALLOW_FORWARDABLE”. The attribute “DISALLOW_ALL_TIX” is used to disable a principal (except in the case of CRYPTOCard principals[1]).

The KDC transaction log files reside under the `tmp/` and `kdc/` directories:

[1] Every user in possession of a CRYPTOCard has an “RB1” instance associated with his or her principal (e.g., username/RB1@FNAL.GOV), which we call a “CRYPTOCard principal”. CRYPTOCard principals are given the “DISALLOW_ALL_TIX” attribute because the credentials obtained via a CRYPTOCard are associated with the principal name “username@FNAL.GOV”.

tmp/ contains the real-time KDC transaction log file, plus recent historical transaction log files, so look there to diagnose a problem in real-time.

kdc/ contains the KDC transaction log files which are at least one day old.

The format of a KDC transaction log file is variable. The diag_user.pl perl script in the tmp/ directory can be used to view the KDC transaction log file for a specific user. For example, if user johndoe is having a problem, try the command (from the directory tmp/):

```
% ./diag_user.pl johndoe
```

This command uses **grep** to search the current KDC transaction log file kdc.log for records with the string johndoe. The command will also output specific error records from the log file that pertain to “johndoe” transactions. The error records appear immediately before the transaction record and are missed if the standard **grep** command is used. Interpreting these KDC error messages is more art than science(!) For example, here is an error that indicates johndoe is using the wrong password (from the tmp/ directory)

```
% ./diag_user.pl johndoe

    ERROR->No such file or directory - pa verify failure
    08:30:31=>AS_REQ from fnkerb.fnal.gov(131.225.68.13) PREAUTH_FAILED
    johndoe@FNAL.GOV for krbtgt/FNAL.GOV@FNAL.GOV, Preauthentication failed
```

The “No such file or directory” output means wrong password. The next record containing “Preauthentication failed” is the message user johndoe receives.

There is another version of the diag_user.pl tool in the princ/ directory. If used from there, the tool defaults to looking at yesterday’s log file.

## 16.9 Changing a Machine’s Node Name

If you need to change the node name of a Kerberized machine, the host and **FTP** service principals and keys, if any, must also be changed. There is no “rename” function on the principal database, so the old service keys must be deleted and new ones added. Request new service principals host/<newname>.<domain> and ftp/<newname>.<domain> using the form at http://www.fnal.gov/cd/forms/extra_kerb_req_form.html. When you get them, follow one of these procedures to change your node name.

### 16.9.1 Using UPS

If you have installed Fermi Kerberos, have **UPS** running and don't mind an interruption, the easiest way to change your node name is to:

1) Change the node name

2) Delete `/etc/krb5.keytab`

3) Run the command: **`ups install-hostkeys kerberos`** and provide the new password(s) when prompted.

### 16.9.2 Using Kerberos Utilities

If you're not running UPS, you'll need to use the native Kerberos utilities. You can avoid interruptions of service during the name change if you want to prepare in advance.

Once you get your new service principals, follow the procedure outlined in section 16.10 *Installing Service Host Keys* to install the new keys.

Then change the node name, and reboot as necessary. You may delete the old host and **FTP** keys from the `keytab` using the **`ktutil`** command:

```
% /usr/krb5/sbin/ktutil

ktutil:  rkt /etc/krb5.keytab

ktutil:  list

                slot KVNO Principal
                ---- ---- -----------------------------------------------
                   1    2     host/oldname.domain@FNAL.GOV
                   2    2      ftp/oldname.domain@FNAL.GOV
                   3    2     host/newname.domain@FNAL.GOV
                   4    2      ftp/newname.domain@FNAL.GOV

ktutil:  delent 2

ktutil:  delent 1
```

Note: Delete entry 2 before entry 1 because they all drop down a slot after **`delent`**. Continue:

```
ktutil:  wkt /etc/krb5.keytab.new

ktutil:  quit

% mv /etc/krb5.keytab.new /etc/krb5.keytab
```

Done!

## 16.10  Installing Service Host Keys

With new host and FTP service principals and their assigned password(s) in hand, log in as *root* and run the **`kadmin`** command as shown below to install the keys (use appropriate values of **`hostname`**, **`domain`** and **`REALM`**). Note that Kerberos clients append the machine's default realm to the principal names typed in the **`kadmin`** command (**`hostname.domain`**). If the default realm of the machine does not match the realm for which the principals/keys were created, then include the **`-r <REALM>`** option.

```
% /usr/krb5/sbin/kadmin -p host/<hostname.domain> \
  -q "ktadd host/<hostname.domain>" [-r <REALM>]
   Enter password: <type in host principal's password>
% /usr/krb5/sbin/kadmin -p ftp/<hostname.domain> \
  -q "ktadd ftp/<hostname.domain>" [-r <REALM>]
   Enter password: <type in ftp principal's password>
```

## 16.11  Static IP vs. DHCP Addresses

You can get host and FTP principals for a DHCP-based machine, but your service principals will work only for your nominal node name (e.g., `host/mynode.dhcp.fnal.gov` and `ftp/mynode.dhcp.fnal.gov`). Whenever that name does not resolve to your current IP address, then the service principal is of no use, and you can't authenticate to your host (you can still authenticate yourself to other hosts). A different machine using your node name cannot impersonate your node or steal Kerberized connections intended for your machine, so there's no risk, just inconvenience. However, if you plan to offer reliable services, a static IP address is the better solution.

## 16.12  Multiple IP Addresses or Node Names

If your machine is configured to have two or more active (static) IP addresses, as long as there's just one node name, you do not need multiple service principals. Just make sure all the IP addresses are listed in DNS. There should be no problems using credentials which have been *forwarded to* such a single-named host.

If you have multiple node names (which are not nicknames), get a host service principal for each name.  This will take care of telnet and the r-commands. FTP will not work properly under these circumstances, and credentials forwarded to such a host will be only partly usable.

## 16.13  Laptops

The feature that sets laptops apart as regards authentication is the fact that they may have different host names and/or IP addresses depending on where they’re being used.  Install the Kerberos product on it as you would on any other machine, but first decide whether you want a static IP address or if you want to use DHCP.